Initial Setup

This chapter contains the following sections:

For Next Steps, See...

This table provides a list of additional documents that are useful references along with the *Cisco APIC Getting Started Guide*. These Cisco APIC documents and others are available at the APIC documents landing page.

Tip To find documentation for a specific Cisco APIC feature, type the feature name in the **Choose a Topic** box in the APIC documents landing page.

Documents
Application Centric Infrastructure Fabric Hardware Installation Guide
Cisco APIC Installation, Upgrade, and Downgrade Guide
Cisco APIC Basic Configuration Guide
Cisco APIC Layer 2 Networking Configuration Guide
Cisco APIC Layer 3 Networking Configuration Guide
Cisco APIC Security Configuration Guide
Cisco APIC System Management Configuration Guide

Documents
Cisco ACI Virtualization Guide
Cisco Application Centric Infrastructure Fundamentals
Cisco APIC Layer 4 to Layer 7 Services Deployment Guide

Most of these links take you to the section of the documentation landing page that contains the specified document. Click the arrow at the right end of the section title to expand the document list for that section, then find the document for your release.

If the document for a release does not exist, the document for the previous release applies. For example, the *Cisco APIC System Management Configuration Guide* was not republished for the 5.0 releases because there are no changes from the 4.2 releases. Therefore, you should use the document for the 4.2 releases.

Simplified Approach to Configuring in Cisco APIC

Cisco APIC supports a simplified approach to configuring the ACI with an additional NX-OS style CLI interface. The existing methods of configuration using REST API and the GUI are supported as well.

In addition to the simple approach available for network administrators and other users of the NX-OS style CLI, there is intelligence embedded in this approach as compared to the GUI or the REST API. In several instances, the NX-OS style CLI can create the ACI model constructs implicitly for a user's ease of use, and they also provide validations to ensure consistency in configuration. This functionality reduces and prevents faults.

For further details about configurations and tasks, see the *Cisco APIC Basic Configuration Guide* and the *Cisco APIC NX-OS Style Command-Line Interface Configuration Guide*.

Changing the BIOS Default Password

Cisco Application Policy Infrastructure Controller (APIC) ships with a default BIOS password. The default password is "password". When the boot process starts, the boot screen displays the BIOS information on the console server.

Note The 6.0(2) and later releases support the APIC-L4 and APIC-M4 servers. These servers have a default password of "password" or "Insieme123".

To change the default BIOS password perform the following task:

Step 1 During the BIOS boot process, when the screen displays **Press <F2> Setup**, press **F2**.
The **Entering Setup** message displays as it accesses the setup menu.

Step 2 At the **Enter Password** dialog box, enter the current password.

Note The default is "password".

The 6.0(2) and later releases support the APIC-L4 and APIC-M4 servers. These servers have a default password of "password" or "Insieme123".

Step 3 In the **Setup Utility**, choose the **Security** tab, and choose **Set Administrator Password**.

Step 4 In the **Enter Current Password** dialog box, enter the current password.

Step 5 In the **Create New Password** dialog box, enter the new password.

Step 6 In the **Confirm New Password** dialog box, re-enter the new password.

Step 7 Choose the **Save & Exit** tab.

Step 8 In the **Save & Exit Setup** dialog box, choose **Yes**.

Step 9 Wait for the reboot process to complete.
The updated BIOS password is effective.

About the APIC

The Cisco Application Centric Infrastructure (ACI) is a distributed, scalable, multitenant infrastructure with external end-point connectivity controlled and grouped through application-centric policies. The Application Policy Infrastructure Controller (APIC) is the unified point of automation, management, monitoring, and programmability for the ACI. The APIC supports the deployment, management, and monitoring of any application anywhere, with a unified operations model for the physical and virtual components of the infrastructure. The APIC programmatically automates network provisioning and control that is based on the application requirements and policies. It is the central control engine for the broader cloud network; it simplifies management and allows flexibility in how application networks are defined and automated. It also provides northbound Representational State Transfer (REST) APIs. The APIC is a distributed system that is implemented as a cluster of many controller instances.

Setting up the Cisco APIC

This section describes how to establish a local serial connection to the Cisco APIC server to begin the initial basic configuration. For additional connection information, including instructions on connecting to the server remotely for setup, refer to "Initial Server Setup" in the *Cisco APIC M3/L3 Server Installation and Service Guide*.

Initial Connection

The Cisco APIC M3/L3 Server operates on a Cisco Integrated Management Controller (CIMC) platform. You can make an initial connection to the CIMC platform using one of these methods:

- Use a KVM cable (Cisco PID N20-BKVM) to connect a keyboard and monitor to the KVM connector on the front panel of the server.
- Connect a USB keyboard and VGA monitor to the corresponding connectors on the rear panel of the server.

Note You cannot use the front panel VGA and the rear panel VGA at the same time.

You can make a serial connection using one of the following methods. Two of these methods require a configuration change in the CIMC:

Note You cannot use more than one of these methods simultaneously.

- Use the DB9 connector of the KVM cable
- Use the rear panel RJ-45 console port (after enabling in the CIMC)
- Connect by Serial-over-LAN (SoL) (after enabling in the CIMC)

The default connection settings from the factory are:

- The serial port baud rate is 115200
- The RJ-45 console port located on the rear panel is disabled in the CIMC
- SoL is disabled in the CIMC

The following are additional notes about serial access:

- If you are using a Cisco Integrated Management Controller (CIMC) for your setup, setup the CIMC first, and then access the Cisco APIC through the CIMC KVM or continue to access the Cisco APIC locally through the rear panel USB/VGA port. If you choose the CIMC KVM access, you will have remote access available later which is required during operations.
- If you are using the RJ-45 console port, connect to CIMC using SSH and enable the SoL port using the following commands:

```
scope sol
  set enabled yes
  set baud-rate 115200
  commit
  exit
```

  After enabling SoL, enter the command **connect host** to access the APIC console.

Note When using SoL, physically disconnect the rear panel RJ-45 console port.

Initial Cisco APIC Setup

When the Cisco Application Policy Infrastructure Controller (Cisco APIC) is launched for the first time, the Cisco APIC console presents a series of initial setup options. For many options, you can press **`Enter`** to choose the default setting that is displayed in brackets. At any point in the setup dialog, you can restart the dialog from the beginning by pressing **`Ctrl-C`**.

Important Notes

- If the UNIX user ID is not explicitly specified in the response from the remote authentication server, then some Cisco APIC software releases assign a default ID of 23999 to all users. If the response from the remote authentication server fails to specify a UNIX ID, all users will share the same ID of 23999 and this can result in the users being granted higher or lower privileges than the configured privileges through the RBAC policies on the Cisco APIC.
- Cisco recommends that you assign unique UNIX user IDs in the range of 16000 to 23999 for the AV Pairs that are assigned to the users when in Bash shell (using SSH, Telnet, or Serial/KVM consoles). If a situation arises where the Cisco AV Pair does not provide a UNIX user ID, the user is assigned a user ID of 23999 or similar number from the range that also enables the user's home directories, files, and processes accessible to the remote users with a UNIX ID of 23999.

  To ensure that your remote authentication server does not explicitly assign a UNIX ID in its **cisco-av-pair** response, open an SSH session to the Cisco APIC and log in as an administrator (using a remote user account). Once logged in, run the following commands (replace **userid** with the username that you logged in with):

  - **admin@apic1: remoteuser-userid> cd /mit/uni/userext/remoteuser-userid**
  - **admin@apic1: remoteuser-userid> cat summary**

- Cisco recommends against modifying any parameters using CIMC. If there are any issues, ensure that the default setting for CIMC management node is **Dedicated Mode** and not **Shared**. If **Dedicated Mode** is not used, it can prevent the discovery of fabric nodes.
- Do not upgrade software or firmware using the CIMC user interface, XML, or SSH interfaces unless the modified property and software or firmware version are supported with your specific Cisco APIC version.
- Set the NIC mode to **Dedicated**, when setting up the CIMC, in the CIMC Configuration Utility. After the CIMC is configured, in the CIMC GUI, verify that you have the following parameters set.

Parameters	Settings
LLDP	Disabled on the VIC
TPM Support	Enabled on the BIOS
TPM Enabled Status	Enabled
TPM Ownership	Owned

- Beginning with Release 5.0(2), if you log in to your Cisco APIC using https, and then attempt to log in to the same Cisco APIC using http in the same browser window without first logging out of the Cisco APIC in the https window, you might see the following error message:

  ```
  Need a valid webtoken cookie (named APIC-Cookie) or a signed request with signature in
  the cookie.
  ```

  If this occurs, resolve the issue using either of the following methods:

  - Log out of the Cisco APIC in the https window, or
  - Delete the cookies in the browser window

You should be able to successfully log into the Cisco APIC using http after resolving the issue with either of the methods above.

- During the initial setup, the system will prompt you to select IPv4, or IPv6, or dual stack configuration. Choosing dual stack will enable accessing the Cisco APIC and Cisco Application Centric Infrastructure (Cisco ACI) fabric out-of-band management interfaces with either IPv4 or IPv6 addresses. While the examples in the table below use IPv4 addresses, you can use whatever IP address configuration options you chose to enable during the initial setup.
- A minimum subnet mask of /19 is recommended.
- Connecting the Cisco APIC to the Cisco ACI fabric requires a 10G interface on the ACI-mode leaf switch. You cannot connect the Cisco APIC directly to the Cisco Nexus 9332PQ, Cisco Nexus 93180LC, or Cisco Nexus 9336C-FX2 ACI-mode leaf switches unless you use a 40G to 10G converter (part number CVR-QSFP-SFP10G), in which case the port on the leaf switches will auto-negotiate to 10G without requiring any manual configuration.

Note Starting with Cisco APIC release 2.2(1n), the Cisco Nexus 93180LC leaf switch is supported.

- The fabric ID is set during the Cisco APIC setup and it cannot be changed unless you perform a clean reload of the fabric. To change the fabric ID, export the Cisco APIC configuration, change the sam.config file, and perform a clean reload of the Cisco APIC and leaf switches. Remove the "fvFabricExtConnP" setting from the exported configuration before importing the configuration into the Cisco APIC after the Cisco APIC comes up. All Cisco APICs in a cluster must have the same fabric ID.
- All logging is enabled by default.
- For login and cluster operations, non-default HTTPS port (default is 443) is not supported for layer 3 physical and layer 3 virtual APICs (on ESXi and AWS). Virtual APICs on ESXi/ AWS are supported from release 6.0(2).

About Cold Standby for a Cisco APIC Cluster

The Cold Standby functionality for a Cisco APIC cluster enables you to operate the Cisco APICs in a cluster in an active/standby mode. In a Cisco APIC cluster, the designated active Cisco APICs share the load and the designated standby Cisco APICs can act as an replacement for any of the Cisco APICs in an active cluster.

An admin user can set up the Cold Standby functionality when the Cisco APIC is launched for the first time. We recommend that you have at least 3 active Cisco APICs in a cluster, and one or more standby Cisco APICs. An admin user must initiate the switch over to replace an active Cisco APIC with a standby Cisco APIC. See the *Cisco APIC Management, Installation, Upgrade, and Downgrade Guide* for more information.

Setup for Active and Standby APIC

Beginning with Cisco Application Policy Infrastructure Controller (APIC) release 6.0(2), for the initial set up and cluster bringup, use the GUI. For more information, see the Bringing up the Cisco APIC Cluster Using the GUI , on page 12 procedure.

Table 1: Setup for Active APIC

Name	Description	Default Value
Fabric name	Fabric domain name	ACI Fabric1
Fabric ID	Fabric ID	1
Number of active controllers	Cluster size	3 **Note** When setting up a Cisco APIC in an active-standby mode, you must have at least 3 active Cisco APICs in a cluster.
POD ID	POD ID	1
Standby controller	Setup standby controller	NO
Controller ID	Unique ID number for the active Cisco APIC instance.	Valid range: 1-32
Standalone APIC Cluster	Is the Cisco APIC cluster not directly connected to the Fabric, but connected by a layer 3 inter-pod network (IPN). This feature is available only on Cisco APIC release 5.2(1) and later.	NO See the knowledge base article *Deploying APIC Cluster Connectivity to the Fabric Over a Layer 3 Network* for additional setup instructions.
Controller name	Active controller name	apic1
IP address pool for tunnel endpoint addresses	Tunnel endpoint address pool	10.0.0.0/16 This value is for the infrastructure virtual routing and forwarding (VRF) only. This subnet should not overlap with any other routed subnets in your network. If this subnet does overlap with another subnet, change this subnet to a different /16 subnet. The minimum supported subnet for a 3 Cisco APIC cluster is /23. If you are using Release 2.0(1) the minimum is /22. The 172.17.0.0/16 subnet is not supported for the infra TEP pool due to a conflict of address space with the docker0 interface. If you must use the 172.17.0.0/16 subnet for the infra TEP pool, you must manually configure the docker0 IP address to be in a different address space in each Cisco APIC before you attempt to put the Cisco APICs in a cluster.

Name	Description	Default Value
VLAN ID for infrastructure network[1]	Infrastructure VLAN for Cisco APIC-to-switch communication including virtual switches **Note** Reserve this VLAN for Cisco APIC use only. The infrastructure VLAN ID must not be used elsewhere in your environment and must not overlap with any other reserved VLANs on other platforms.	
IP address pool for bridge domain multicast address (GIPo)	IP addresses used for fabric multicast. For Cisco APIC in a Cisco ACI Multi-Site topology, this GIPo address can be the same across sites.	225.0.0.0/15 Valid range: 225.0.0.0/15 to 231.254.0.0/15, prefixlen must be 15 (128k IPs)
IPv4/IPv6 addresses for the out-of-band management	IP address that you use to access the Cisco APIC through the GUI, CLI, or API. This address must be a reserved address from the VRF of a customer	—
IPv4/IPv6 addresses of the default gateway	Gateway address for communication to external networks using out-of-band management	—
Management interface speed/duplex mode	Interface speed and duplex mode for the out-of-band management interface	auto Valid values are as follows • auto • 10baseT/Half • 10baseT/Full • 100baseT/Half • 100baseT/Full • 1000baseT/Full

Name	Description	Default Value
Strong password check	Check for a strong password	[Y]
Password	Password of the system administrator This password must be at least 8 characters with one special character.	—

[1] To change the VLAN ID after the initial APIC setup, export your configurations, rebuild the fabric with a new infrastructure VLAN ID and import the configurations so that the fabric does not revert to the old infrastructure VLAN ID. See the KB article about *Using Export and Import to Recover Configuration State*.

Table 2: Setup for Standby APIC

Name	Description	Default Value
Fabric name	Fabric domain name	ACI Fabric1
Fabric ID	Fabric ID	1
Number of active controllers	Cluster size	3 **Note** When setting up Cisco APIC in an active-standby mode, you must have at least 3 active Cisco APICs in a cluster.
POD ID	ID of the POD	1
Standby controller	Setup standby controller	Yes
Standby Controller ID	Unique ID number for the standby Cisco APIC instance	Recommended range: >20
Controller name	Standby controller name	NA
IP address pool for tunnel endpoint addresses	Tunnel endpoint address pool	10.0.0.0/16 This value is for the infrastructure virtual routing and forwarding (VRF) only. This subnet should not overlap with any other routed subnets in your network. If this subnet does overlap with another subnet, change this subnet to a different /16 subnet. The minimum supported subnet for a 3 Cisco APIC cluster is /23. If you are using Release 2.0(1) the minimum is /22.

Name	Description	Default Value
VLAN ID for infrastructure network[2]	Infrastructure VLAN for Cisco APIC-to-switch communication including virtual switches **Note** Reserve this VLAN for Cisco APIC use only. The infrastructure VLAN ID must not be used elsewhere in your environment and must not overlap with any other reserved VLANs on other platforms.	
IPv4/IPv6 addresses for the out-of-band management	IP address that you use to access the Cisco APIC through the GUI, CLI, or API. This address must be a reserved address from the VRF of a customer	—
IPv4/IPv6 addresses of the default gateway	Gateway address for communication to external networks using out-of-band management	—
Management interface speed/duplex mode	Interface speed and duplex mode for the out-of-band management interface	auto Valid values are as follows • auto • 10baseT/Half • 10baseT/Full • 100baseT/Half • 100baseT/Full • 1000baseT/Full
Strong password check	Check for a strong password	[Y]
Password	Password of the system administrator This password must be at least 8 characters with one special character.	—

[2] To change the VLAN ID after the initial APIC setup, export your configurations, rebuild the fabric with a new infrastructure VLAN ID and import the configurations so that the fabric does not revert to the old infrastructure VLAN ID. See the KB article about *Using Export and Import to Recover Configuration State*.

Example

The following example output shows the initial setup dialog as displayed on the console.

Note Instead of using the **APIC Cluster Bringup** GUI, you can bootstrap and bringup the cluster using REST APIs. For more information, see the *Cisco APIC REST API Configuration Guide*.

Beginning with Cisco APIC release 6.0(2), questions in the example output are not included. For bootstrapping, and bringing up the Cisco APIC cluster, use the GUI. For details, see the Bringing up the Cisco APIC Cluster Using the GUI , on page 12 procedure.

```
Cluster configuration ...
  Enter the fabric name [ACI Fabric1]:
  Enter the fabric ID (1-128) [1]:
  Enter the number of active controllers in the fabric (1-9) [3]:
  Enter the POD ID (1-9) [1]:
  Is this a standby controller? [NO]:
  Enter the controller ID (1-3) [1]:
  Enter the controller name [apic1]: apic-1
  Enter address pool for TEP addresses [10.0.0.0/16]:
  Note: The infra VLAN ID should not be used elsewhere in your environment
        and should not overlap with any other reserved VLANs on other platforms.
  Enter the VLAN ID for infra network (2-4094): 3914
  Enter address pool for BD multicast addresses (GIPO) [225.0.0.0/15]:

Out-of-band management configuration ...
  Enable IPv6 for Out of Band Mgmt Interface? [N]:
  Enter the IPv4 address [192.168.10.1/24]: 172.31.1.2/24
  Enter the IPv4 address of the default gateway [None]: 172.31.1.1
  Enter the interface speed/duplex mode [auto]:

admin user configuration ...
  Enable strong passwords? [Y]:
  Enter the password for admin:

  Reenter the password for admin:

Cluster configuration ...
  Fabric name: ACI Fabric1
  Fabric ID: 1
  Number of controllers: 3
  Controller name: apic-1
  POD ID: 1
  Controller ID: 1
  TEP address pool: 10.0.0.0/16
  Infra VLAN ID: 3914
  Multicast address pool: 225.0.0.0/15

Out-of-band management configuration ...
  Management IP address: 172.31.1.2/24
  Default gateway: 172.31.1.1
  Interface speed/duplex mode: auto

admin user configuration ...
```

```
  Strong Passwords: Y
  User name: admin
  Password: ********

The above configuration will be applied ...

Warning: TEP address pool, Infra VLAN ID and Multicast address pool
         cannot be changed later, these are permanent until the
         fabric is wiped.

Would you like to edit the configuration? (y/n) [n]:
```

Bringing up the Cisco APIC Cluster Using the GUI

Beginning with Cisco APIC release 6.0(2), the initial cluster set up and bootstrapping procedure has been simplified with the addition of GUI screen(s) for cluster bring up. The **APIC Cluster Bringup** GUI supports virtual and physical APIC platforms. The virtual APICs (deployed using ESXi or AWS), and physical APICs can be connected to the ACI fabric directly to the leaf switches or remotely attached through a Layer 3 network. The GUI supports both the scenarios. A major advantage of using the **APIC Cluster Bringup** GUI is that, you do not need to enter the parameters for every APIC in a cluster. One APIC can relay the information to the other APICs of the cluster.

Alternatively, you can perform the initial setup and cluster bringup using the REST APIs. See the *Getting Started* section of the APIC REST API Configuration Procedures guide.

Before you begin

- For virtual APIC on ESXi, ensure to complete the deployment of the Cisco APIC VM using the OVF template on the VMware vCenter GUI. For a three-node cluster, configure three VMs with the management IP address, gateway, and admin passwords. The number of VMs is dependent on the size of the Cisco APIC cluster.
- For virtual APIC on AWS, ensure to complete the deployment of the Cisco APIC VM using the cloud formation template (CFT) on the AWS GUI. AWS allocates IP addresses dynamically from the out-of-band (OOB)/infra/inband subnets accordingly, to correspond with the network adapters of the virtual APIC's EC2 instance.
- For virtual APICs (deployed using AWS/ ESXi), ensure that the admin password(s) are the same for all the Cisco APICs in a cluster.
- For the physical APIC cluster, configure the OOB address for APIC 1. Ensure that the CIMC addresses of APICs 2 to *N* (where N is the cluster size) are reachable via the OOB address of APIC 1.
- Connectivity between out-of-band and the CIMC is mandatory.

Limitations:

- No support for IPv6 addresses on virtual APICs deployed using AWS.
- For login and cluster operations, non-default HTTPS port (default is 443) is not supported for remotely-attached Cisco APICs (physical and virtual).

Step 1 Log in to the APIC 1 using *https://APIC1-IP*.

a) For virtual APICs:

If you have completed the deployment of virtual APICs using ESXi (OVF template) or remote AWS (CFT), then you see output on the VM console similar to the following example:

```
System pre-configured successfully.
Use: https://172.31.1.2 to complete the bootstrapping.
```

The IP address to access the bootstrapping GUI (**APIC Cluster Bringup**) is explicitly indicated, as shown in the example. You can proceed to step 2.

After deploying Cisco APIC on AWS, keep the OOB management IP address handy to access the **Cluster Bringup** GUI. You can get the OOB management IP address from the **Stacks Outputs** tab on the AWS GUI.

b) For physical APICs:

Log in to the APIC 1 KVM console using the CIMC; you will see a screen as shown below:

```
APIC Version: 6.0(2a)
Welcome to Cisco APIC Setup Utility
Press Enter Or Input JSON string to bootstrap your APIC node.
```

If you see only a black screen on the KVM, connect to the CIMC using SSH and use serial over LAN (SoL) ("connect host") to connect to the console.

On APIC 1, press **Enter** and provide the requested information. The IP address to access the bootstrapping GUI (**APIC Cluster Bringup**) is explicitly indicated.

```
admin user configuration ...
  Enter the password for admin [None]:
  Reenter the password for admin [None]:
Out-of-band management configuration ...
  Enter the IP Address [192.168.10.1/24]: 172.20.7.79/23
  Enter the IP Address of default gateway [192.168.10.254]: 172.20.6.1
Would you like to edit the configuration? (y/n) [n]:
System pre-configured successfully.
Use: https://172.20.7.79 to complete the bootstrapping
```

The IP addresses displayed above are examples. The IP addresses will vary based on your deployment.

Step 2 Using the OOB address, log in to the **APIC Cluster Bringup** GUI. The GUI screen has four parts. Enter the details in the following screens:

- Connection Type
- Cluster Details
- Controller Registration
- Summary

Each of the above screens are discussed in detail in the subsequent steps. The screens are marked as steps with sequential numbers: 1, 2, 3, and 4; after you have entered and saved the required details in each of these screens, the number is replaced with a tick-mark.

Step 3 The first step is entering the **Connection Type** information. In the **Connection Type** screen, choose the type of connection between the APIC and the fabric.

The options are:

- Directly connected to leaf switches (ACI fabric)
- Remotely attached through a Layer 3 network

If it is virtual APIC using AWS, the system detects that the APIC is remotely-attached through a Layer 3 network and proceeds directly to the **Cluster Details** screen.

Step 4 Click **Next**.

Step 5 The second step is entering the **Cluster Details**. Enter the fabric-level details in the **Cluster Details** screen.

- Fabric Name: Enter a name for the fabric.
- Cluster Size: The default cluster size displayed is "3", which is the recommended minimum cluster size. You can modify this value, based on your cluster size. The supported values are 1, 3, 4, 5, 6, 7, 8, and 9.
- GiPo Pool: Enter the IP address used for fabric multicast. The default address is 225.0.0.0/15. The range is from 225.0.0.0/15 to 231.254.0.0/15. The prefixlen must be 15 (128k IP addresses).

  You cannot change this value after you have completed the configuration. Having to modify this value requires a wipe of the fabric.
- Pod ID: (applicable only for directly connected APICs (virtual and physical)) the pod ID is displayed. If this is your first APIC, "1" is auto-populated. Subsequent APICs of the cluster can be associated with any pod number.

  For a remotely-attached APICs, pod is 0.
- TEP Pool: (applicable only for directly connected APICs (ESXi virtual APIC and physical APIC)) enter the subnet of addresses used for internal fabric communication. The size of the subnet used will impact the scale of your pod.

  You can not change this value after you have completed the configuration. Having to modify this value requires a wipe of the fabric.
- Infrastructure VLAN: Enter the VLAN ID for fabric connectivity (infra VLAN). This VLAN ID should be allocated solely to ACI, and not used by any other legacy device(s) in your network. Default value is 3914. The range is from 0 to 4093.

  You can not change this value after you have completed the configuration. Having to modify this value requires a wipe of the fabric.
- Enable IPv6 on APICs (not applicable for virtual APIC on AWS): Put a check in this box if you want to enable IPv6 addresses for out-of-band management.

Step 6 Click **Next**.

Step 7 The third step is entering the **Controller Registration** details. Click **Add Controller** to add the first APIC (of the cluster). Enter the following details:

- Controller Type: The bootstrapping procedure auto-detects the deployment for which the configuration is being carried out. Based on that, either **Virtual** or **Physical** is chosen. The options displayed for the virtual and physical controller types are discussed in substeps (a) and (b), respectively. Follow either of these substeps based on the controller type.

a) When the Controller Type is **Virtual**:

- Virtual Instance: The management IP used to access the APIC cluster bringup GUI. Only for the first APIC, this IP address is auto-populated. For the nodes that you subsequently add to the cluster, you will need to enter the management IP address and click **Validate**.

  The management IP addresses are defined during the deployment of the VMs using ESXi/AWS. As mentioned in the prerequisites, keep all the required IP addresses handy while bringing up the cluster.
- General pane

    - Name: User-defined name for the controller.
    - Controller ID: The ID is auto-populated. If this is the first APIC of the cluster, the ID is "1". If you are adding the second controller of the cluster, "2" is auto-populated (and so on).
    - Pod ID: (Applicable only for *directly connected* virtual APIC on ESXi) The pod ID is auto-populated for APIC 1 of the cluster. For subsequent controllers of the cluster, enter a value. The range is from 1 to 128.
    - Serial Number: The serial number of the virtual machine is auto-populated.

- Out of Band Network pane
    - IPv4 Address: The IP address is displayed (as defined during the deployment).
    - IPv4 Gateway: The IP address is displayed (as defined during the deployment).

  If you have enabled IPv6 addresses for OOB management earlier (step 5), enter the IPv6 address and gateway.

- Infra L3 Network pane (this pane is displayed only if the **Connection Type** that you chose earlier is *Remotely attached through an L3 network*.
    - IPv4 Address: Enter the infra network address.
    - IPv4 Gateway: Enter the IP address of the gateway.
    - VLAN: (Applicable only for *remotely attached* virtual APIC- ESXi) Enter the interface VLAN ID to be used.

  The Infra L3 Network pane does not display when you deploy the virtual APIC using AWS.

After you have entered and saved the first APIC details, click **Add Controller** on the **Controller Registration** screen to add another APIC to the cluster.

b) When the Controller Type is **Physical**:

- CIMC Details pane
    - IP Address: The CIMC IP address. Only for the first Cisco APIC, this IP address is auto-populated. When you add more controllers to the cluster, you need to enter the CIMC IP addresses.
    - Username: The username to access the CIMC. The username is auto-populated (for the first controller and subsequent controllers).
    - Password: Enter the password to access CIMC. For the first controller, the password is auto-populated. For the subsequent controllers, enter the password.
    - Click **Validate**. *Validation success* is displayed on successful authentication.

      If the CIMC is unreachable from the Cisco APIC out of band management IP address due to the CIMC NIC mode settings, change the NIC mode or enter JSON strings to perform the bootstrap.

- General pane
    - Name: Enter a name for the controller.
    - Controller ID: If it is the first controller of the cluster, "1" is auto-populated. If it is the second controller, "2" is auto-populated, and so on (increasing order).

  - Pod ID: (applicable only for a directly-connected APIC) the pod ID is auto-populated for APIC 1 of the cluster. For subsequent controllers of the cluster, enter a value. The range is from 1 to 128.
  - Serial Number: The serial number is auto-populated (for APICs 1 to N, where N is the cluster size) after CIMC validation.

    APIC 1 verifies the reachability of the CIMC IP addreses and also captures the serial number of the new APICs.

- Out of Band Network pane
  - IPv4 Address: For APIC 1, the address is auto-populated. For subsequent APICs, enter the IP address (as defined during the deployment).
  - IPv4 Gateway: For APIC 1, the gateway address is auto-populated. For subsequent APICs, enter the IP address (as defined during the deployment).

  If you have enabled IPv6 addresses for OOB management earlier (step 5), enter the IPv6 address and gateway.

- Infra L3 Network pane (this pane is displayed only if the **Connection Type** that you chose earlier is remotely attached through a Layer 3 network).
  - IPv4 Address: Enter the infra network IP address.
  - IPv4 Gateway: Enter the infra network IP address of the gateway.
  - VLAN: Enter a VLAN ID.

On the **Controller Registration** screen, after you have entered and saved the first APIC details, click **Add Controller** to add another APIC to the cluster.

(Optional, applicable only for virtual APICs) On the **Controller Registration** screen, put a check in the **Import existing security certificates** box to import existing security certificates for fabric recovery in virtual APICs. After putting a check in the box, enter the required details in the following fields:

- The **Remote Server IP Address** which contains the configuration file.
- The **Remote Path** which contains the configuration file.
- The configuration **File Name**.
- The **AES Encryption Passphrase** which was earlier used while backing up the configuration. The backup configuration file is linked to this key (passphrase).
- Choose the **Protocol**. The choices are:
  - **FTP**
  - **SFTP**
  - **SCP**
- **Remote Port**
- (applicable only for SFTP and SCP **Protocols**) Choose the **Authentication Type**. The choices are:
  - **Use Password**
  - **Use SSH Private Key Files**

- The **Username** to access the remote server.
- The **Password** to authenticate access to the remote server.
- (applicable only for Use SSH Private Key Files **Authentication Type**) Enter the **SSH Key Contents** here.
- (applicable only for Use SSH Private Key Files **Authentication Type**) Specify the **SSH Key Passphrase** used for encrypting the private key.

  For details about the Import/Export procedure, see the Cisco ACI Configuration Files: Import and Export document.

The **Import existing security certificates** is applicable only for virtual APICs (deployed using AWS/ ESXi). Physical APICs have in-built certificates. However, in case of virtual APICs, when you are restoring using backup configuration to recover the fabric, the existing security certificates can be re-used.

Step 8 Click **Next**.

The **Next** button is disabled until all the controllers for a cluster are added. This is defined by the value you have entered for **Cluster Size** in the **Cluster Details** screen.

You can use the **Back** button to navigate to an earlier screen. After adding an APIC, click **Edit Details** to edit the information for an APIC. Except the first APIC, you can delete the other controllers, if required, by clicking the delete icon.

Step 9 In the **Summary** screen, review the updates, and click **Deploy**.

Step 10 The **Cluster Status** page is displayed, which shows the current status of the cluster formation. Wait for a few minutes after which you will be automatically redirected to the standard Cisco APIC GUI.

Provisioning IPv6 Management Addresses on APICs

IPv6 management addresses can be provisioned on the Cisco Application Policy Infrastructure Controller (APIC) at setup time or through a policy once the Cisco APIC is operational. Pure IPv4, pure IPv6, or dual stack (that is, both IPv6 and IPv4 addresses) are supported. A snippet of a typical setup screen that describes how to set up dual stack (IPv6 and IPv4) addresses for out-of-band management interfaces during the setup is given below. However, the following questionnaire is applicable for releases prior to 6.0(2). From Cisco APIC release 6.0(2), the cluster bringup is using the GUI as detailed above.

```
Cluster configuration …

  Enter the fabric name [ACI Fabric1]:
  Enter the number of controllers in the fabric (1-9) [3]:
  Enter the controller ID (1-3) [1]:
  Enter the controller name [apic1]: infraipv6-ifc1
  Enter address pool for TEP addresses [10.0.0.0/16]:
  Note: The infra VLAN ID should not be used elsewhere in your environment
        and should not overlap with any other reserved VLANs on other platforms.
  Enter the VLAN ID for infra network (1-4094): 3914
  Enter address pool for BD multicast addresses (GIPO) [225.0.0.0/15]:

Out-of-band management configuration ...
  Enable IPv6 for Out of Band Mgmt Interface? [N]: Y (Enter Y to Configure IPv6 Address for
 Out of Band Management Address)
  Enter the IPv6 address [0:0:0:0:0:ffff:c0a8:a01/40]: 2001:420:28e:2020:0:ffff:ac1f:88e4/64
 (IPv6 Address)
  Enter the IPv6 address of the default gateway  [None]: 2001:420:28e:2020:acc:68ff:fe28:b540
 (IPv6 Gateway)
  Enable IPv4 also for Out of Band Mgmt Interface? [Y]: (Enter Y to Configure IPv4 Address
 for Out of Band Management Address)
  Enter the IPv4 address [192.168.10.1/24]: 172.31.136.228/21 (IPv4 Address)
  Enter the IPv4 address of the default gateway [None]: 172.31.136.1 (IPv4 Gateway)
  Enter the interface speed/duplex mode [auto]:

admin user configuration ...
  Enable strong passwords? [Y]:
  Enter the password for admin:

  Reenter the password for admin:
```

Note While using the **APIC Cluster Bringup** GUI, you can select the **Enable IPv6** option to use IPv6 addresses.

Accessing the GUI

Step 1 Open one of the supported browsers:

- Chrome version 59 (at minimum)
- Firefox version 54 (at minimum)
- Internet Explorer version 11 (at minimum)
- Safari version 10 (at minimum)

Note A known issue exists with the Safari browser and unsigned certificates. Read the information presented here before accepting an unsigned certificate for use with WebSockets. When you access the HTTPS site, the following message appears:

“Safari can’t verify the identity of the website APIC. The certificate for this website is invalid. You might be connecting to a website that is pretending to be an APIC, which could put your confidential information at risk. Would you like to connect to the website anyway?”

To ensure that WebSockets can connect, you must do the following:

Click **Show Certificate**.

Choose **Always Trust** in the three drop-down lists that appear.

If you do not follow these steps, WebSockets will not be able to connect.

Step 2 Enter the URL: **https://***mgmt_ip-address*

Use the out-of-band management IP address that you configured during the initial setup. For example, https://192.168.10.1.

Note Only https is enabled by default. By default, http and http-to-https redirection are disabled.

Note If you see the following error message when logging into your Cisco APIC:

```
Need a valid webtoken cookie (named APIC-Cookie) or a signed request with signature in the
cookie.
```

This is due to a known issue that occurs when you are logging into a Cisco APIC using both https and http. See the "Important Notes" section in Setting up the Cisco APIC , on page 3 for more information on this issue and the workaround.

Step 3 When the login screen appears, enter the administrator name and password that you configured during the initial setup.

Step 4 In the **Domain** field, from the drop-down list, choose the appropriate domain that is defined.

If multiple login domains are defined, the **Domain** field is displayed. If the user does not choose a domain, the DefaultAuth login domain is used for authentication by default. This may result in login failure if the username is not in the DefaultAuth login domain.

What to do next

To learn about the features and operation of the Application Centric Infrastructure fabric and the Application Policy Infrastructure Controller, see the available white papers and the *Cisco Application Centric Infrastructure Fundamentals Guide*.

Accessing the REST API

By using a script or a browser-based REST client, you can send an API POST or GET message of the form: **https:**//*apic-ip-address*/**api**/*api-message-url*

Use the out-of-band management IP address that you configured during the initial setup.

Note

- Only https is enabled by default. By default, http and http-to-https redirection are disabled.
- You must send an authentication message to initiate an API session. Use the administrator login name and password that you configured during the initial setup.

Accessing the NX-OS Style CLI

You can access the APIC NX-OS style CLI either directly from a terminal or through the APIC GUI.

For information about using the NX-OS style CLI commands, see the *Cisco APIC NX-OS Style Command-Line Interface Configuration Guide* and the *Cisco APIC NX-OS Style CLI Command Reference*.

Guidelines and Restrictions for the APIC NX-OS Style CLI

- The CLI is supported only for users with administrative login privileges.

- The APIC NX-OS style CLI uses similar syntax and other conventions to the Cisco NX-OS CLI, but the APIC operating system is not a version of Cisco NX-OS software. Do not assume that a Cisco NX-OS CLI command works with or has the same function on the APIC CLI.
- If FIPS is enabled in the Cisco ACI setups, then SHA256 support is mandatory on the SSH Client. Additionally, to have the SHA256 support, the openssh-client must be running version 6.6.1 or higher.
- In releases earlier than Cisco APIC Release 1.2, the default CLI was a Bash shell with commands to directly operate on managed objects (MOs) and properties of the Management Information Model. Beginning with Cisco APIC Release 1.2, the default CLI is a NX-OS style CLI. The object model CLI is available by typing the **bash** command at the initial CLI prompt.

Accessing the NX-OS Style CLI from a Terminal

Step 1 From a secure shell (SSH) client, open an SSH connection to APIC at *username@ip-address*.

Use the administrator login name and the out-of-band management IP address that you configured during the initial setup. For example, admin@192.168.10.1.

Step 2 When prompted, enter the administrator password.

What to do next

When you enter the NX-OS style CLI, the initial command level is the EXEC level. You can stay in EXEC mode or you can type **configure** to enter global configuration mode. In any mode, type **?** to see the available commands.

For information about using the NX-OS style CLI commands, see the *Cisco APIC NX-OS Style Command-Line Interface Configuration Guide* and the *Cisco APIC NX-OS Style CLI Command Reference*.

Accessing the NX-OS Style CLI from the GUI

Step 1 From the menu bar, choose **System** > **Controllers**.

Step 2 In the navigation pane, click **Controllers**.

Step 3 Right-click the desired APIC and choose **Launch SSH**.

Step 4 Follow the displayed instructions to open an SSH session to the selected controller.

What to do next

When you enter the NX-OS style CLI, the initial command level is the EXEC level. You can stay in EXEC mode or you can type **configure** to enter global configuration mode. In any mode, type **?** to see the available commands.

For information about using the NX-OS style CLI commands, see the *Cisco APIC NX-OS Style Command-Line Interface Configuration Guide* and the *Cisco APIC NX-OS Style CLI Command Reference*.

Accessing the Object Model CLI

Note In releases earlier than Cisco APIC Release 1.2, the default CLI was a Bash shell with commands to directly operate on managed objects (MOs) and properties of the Management Information Model. Beginning with Cisco APIC Release 1.2, the default CLI is a NX-OS style CLI. The object model CLI is available by typing the **bash** command at the initial CLI prompt.

Step 1 From a secure shell (SSH) client, open an SSH connection to *username@ip-address*.

Use the administrator login name and the out-of-band management IP address that you configured during the initial setup. For example, `ssh admin@192.168.10.1`.

Step 2 When prompted, enter the administrator password that you configured during the initial setup.

You are now in the NX-OS style CLI for APIC.

Step 3 Type **bash** to enter the object model CLI.

Step 4 To return to the NX-OS style CLI, type **exit**.

This example shows how to enter the object model CLI and how to return to the NX-OS style CLI:

```
$ ssh admin@192.168.10.1
Application Policy Infrastructure Controller
admin@192.168.10.1's password: cisco123
apic#             <---- NX-OS style CLI prompt
apic# bash
admin@apic1:~>    <---- object model CLI prompt
admin@apic1:~> exit
apic#
```

What to do next

Every user must use the shared directory called `/home`. This directory gives permissions for a user to create directories and files; files created within `/home` inherit the default umask permissions and are accessible by the user and by root. We recommend that users create a `/home/userid` directory to store files, such as `/home/jsmith`, when logging in for the first time.

For more information about accessing switches using the ACI CLI using modes of operation such as BASH or VSH, see the *Cisco APIC Command Line Interface User Guide* and the *Cisco ACI Switch Command Reference*.

For detailed information about configuring the APIC CLI, see the *Cisco APIC Object Model Command Line Interface User Guide*.